UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,491	06/15/2001	Yaron Goland	3382-53699	8148

26119 7590 04/05/2007

KLARQUIST SPARKMAN LLP
121 S.W. SALMON STREET
SUITE 1600
PORTLAND, OR 97204

EXAMINER	
SHAW, YIN CHEN	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/882,491	GOLAND, YARON	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 January 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 01/11/2007.

2. Claims 1-20 are as original.

3. Claims 1-20 have been examined and rejected.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al, US Patent No. 6772331B1, hereinafter "Hind", in view of Dondeti et al, US Patent No. 7013389, hereinafter "Dondeti".

6. As per claim 1:

Hind teaches "A branding process to establish a trust web of networked computing devices on an open multi-access network, comprising:

Securely networking a security-uninitialized device with a branding device via a secured network medium" in (Col 9 lines 25-40);

"Electronically imprinting the security-uninitialized device with group membership and cryptographic key data by the branding device via the secured network medium" in (Col 9 lines 25-40), the cryptographic key data for verifying group membership information provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device" in (Col 9 lines 15-60, creating a trust between the devices); and

Initializing the security-uninitialized device to use the cryptographic key data to authenticate group membership of other devices interacting with security-un-initialized device on the open multi-access network, and to provide the security-uninitialized device is a member of the trust web, such that at least some interaction via the open multi-access network with the security-uninitialized device is cryptographically secured to only other devices in the trust web" in (Col 10 lines 18-29, and Col 11 line 5 to Col 12 line 20 and Col 9 lines 35-60). Hind further teaches of having additional fields including user group associations, access control groups in the signed certificate.

However, Hind does not specifically discloses a method of utilizing the group membership information with other branded devices in an open multi-access network.

Nevertheless, Dondeti discloses the "Dual Encryption Protocol for scalable secure group communication" invention, which includes a method of joining a un-initialized device into a group by providing a group membership certificate to the un-initialized device. The initialized device with the group membership certificate can

send the group membership certificate to other member in the group for authentication" in (Col 4 line 57 to Col 5 line 21).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Hind's invention to incorporate Dondeti's teaching to implement the group joining between group members without interposing a central authority.

7. As per claims 2 and 13:

Hind teaches "A branding process to establish cryptographically secured interaction among networked computing devices within a trust group on an open multi-access network, comprising:

securely networking a security-un-initialized device with a branding device via a secured network medium (Col 9 lines 25-40);

transmitting a branding certificate from the branding device to the security-un-initialized device via the secured network medium (Col 9 lines 25-40), the branding certificate instructing that the security-un-initialized device trust the branding device (Col 9 lines 15-60, creating a trust between the devices), the branding certificate further containing key data for verifying certificates provided by other devices on the open multi-access network to the security-un-initialized device are authenticated by the branding device (Col 9 lines 35-60);

transmitting a trust group membership certificate signed by the branding device to the security-un-initialized device via the secured network medium, the trust group

membership certificate containing a signed group name as well as a signed key identifying the security-un-initialized device such that, when the security-un-initialized device sends the trust group certificate to a branded device which is a member of the trust group, the trust group certificate is validated by the branded device, and the branded device verifies that the security-un-initialized device is a member of the trust group of devices referred to by the group name (Col 10 lines 18-29); and

initializing a security resolver of the security-un-initialized device to use the key data of the branding certificate to authenticate other devices interacting with the security-un-initialized device on the open multi-access network are in the trust group (Col 10 lines 18-29, and Col 11 line 5 to Col 12 line 20), and to provide the trust group membership certificate to such other devices as authentication that the security-un-initialized device is a member of the trust group (Col 10 lines 18-29, such that at least some interaction via the open multi-access network with the security-un-initialized device is cryptographically secured to only other devices in the trust group (Col 9 lines 15-60)". Hind further teaches of having additional fields including user group associations, access control groups in the signed certificate.

However, Hind does not specifically discloses a method of utilizing the group membership information with other branded devices in an open multi-access network.

Nevertheless, Dondeti discloses the "Dual Encryption Protocol for scalable secure group communication" invention, which includes a method of joining a un-

initialized device into a group by providing a group membership certificate to the un-initialized device. The group membership certificate also includes group identity and other information to further authenticate the un-initialized device to a group (See Figure 3 & 4 and Col 5 lines 1-20). The initialized device with the group membership certificate can send the group membership certificate to other member in the group for authentication" in Col 4 line 57 to Col 5 line 21).

Therefore; it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Hind's invention to incorporate Dondeti's teaching to implement the group joining between group members without interposing a central authority.

8. As per claim 3:

Hind and Dondeti teach "The branding process of claim 2 wherein securely networking the security-un-initialized and branding devices comprises networking the devices via a limited access network interface of the security-un-initialized device that is separate from the security-un-initialized device's interface to the open multi-access network" (Col 11 lines 5-65).

9. As per claim 4:

Hind and Dondeti teach "The branding process of claim 3 wherein the limited access network interface is of a direct device-to-device wired networking medium (Col 1 line 65 to Col 2 line 1).

10. As per claim 5:

Hind and Dondeti teach "The branding process of claim 3 wherein the limited access network interface is of a directional wireless networking medium" in (Col 1 line 55 to Col 2 line 10).

11. As per claim 6:

Hind and Dondeti teach "The branding process of claim 2 wherein securely networking the security-un-initialized and branding devices comprises: placing transmitter/receivers of the security-un-initialized and branding devices for an omni-directional wireless networking medium into a wave guide and/or Faraday cage; and networking the devices with the wave guide and/or Faraday cage via the omni-directional wireless networking medium" in (Col 1 line 55 to Col 2 line 10).

12. As per claim 7:

Hind and Dondeti teach "The branding process of claim 2 further comprising: transmitting a principal identifier from the branding device to the security-un-

initialized device, the principal identifier providing a cryptographically secured identity to the security-un-initialized device, the principal identifier containing a public/private key pair; and using the public/private key pair to encrypt interaction of the security-un-initialized device with said other devices authenticated to be in the trust group" in (Col 11 lines 5-65).

13. As per claim 8:

Hind and Dondeti teach "The branding process of claim 7 wherein the principal identifier further contains a name for the security-un-initialized device, the process further comprising identifying the security-un-initialized device to human operators using the name" in (Col 12 lines 45-65).

14. As per claim 9:

Hind and Dondeti teach "The branding process of claim 8 further comprising prompting a human user of the branding device to enter the name upon performing the branding process on the security-un-initialized device" in (Col 12 lines 45-65).

15. As per claim 10:

Hind and Dondeti teach "The branding process of claim 2 further comprising initially distributing the security-un-initialized device in a retail channel prior to having the branding process performed on the security-un-initialized device" in (Col 5 lines 25).

16. As per claim 11:

Hind and Dondeti teach "The branding process of claim 10 further comprising upon completion of initializing the security resolver, disallowing the security-un-initialized device from having the branding process again performed on the security-un-initialized device until the now initialized security of the security-un-initialized device is reset" in (Col 13 lines 35-43).

17. As per claim 12:

Hind and Dondeti teach "The branding process of claim 10 further comprising upon completion of initializing the security resolver, allowing the branding process to be performed only via a limited access network interface of the security-un-initialized device" in (Col 4 line 53 to Col 5 line 5).

18. As per claim 14:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: a limited access networking interface; and the security initializer further operational to accept the branding public key when received from the branding device only via the limited access networking interface" in (Col 11 lines 5-45).

19. As per claim 15:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in an initial unbranded state; and a branding reset operational upon activation to return the security initializer to the initial unbranded state" in (Col 13 lines 35-43).

20. As per claim 16:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: a branding mode activator operational to place the networked computing device in a branding mode; and the security initializer further operational to accept the branding public key when received from the branding device via the network interface when in the branding mode" in (Col 11 lines 5-45).

21. As per claim 17:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a trust group membership certificate to provide the trust group membership certificate to other devices via the network interface to attest to membership of the networked computing in the trust group; and the security initializer further operational to receive the trust group membership certificate from the branding device while securely

networked to the networked computing device, and further operational to initialize the security resolver with the trust group membership certificate" in (Col 9 lines 15-65, and Col 10 lines 24-30).

22. As per claim 18:

Hind and Dondeti teach "The networked computing device of claim 13 further comprising: the security resolver further operational when initialized with a public/private key pair to encrypt interaction via the network interface with other devices authenticated as in the trust group using the public/private key pair; and the security initializer further operational to receive the public/private key pair from the branding device while securely networked to the networked computing device, and further operational to initialize the security resolver with the public/private key pair" in (Col 11 lines 5-65).

23. As per claim 19:

Dondeti discloses "The branding process of claim 1, wherein the group membership information comprises a certificate signed by the branding device and containing a signed group name as well as signed information naming the security-un-initialized device such that, when the security-un-initialized device provides the certificate to a branded device which is a member of the trust web, the certificate is validated by the branded device, and the branded device verifies that the security-uniinitialized

device named in the certificate is a member of the trust group of devices referred to by the group name" in (Col 4 line 57 to Col 5 line 21).

24. As per claim 20:

Dondeti discloses "The networked computing device of claim 13, wherein:

Each trust group membership certificate is sent by an other device and each trust group membership certificates comprises:

A signed name for a trust group (Group Name or group ID);

A signed identifier (host public key, Host ID) for the other devices sending the trust group membership certificate" in (Figure 1, 3); and

"The security resolver is configured to authenticate trust group membership certificates by:

Authenticating, from the trust group membership certificate, the signed name for the trust group and the signed identifier for the other device sending the trust group membership certificate using the branding public key" in (Col 6 lines 10-55); and

Wherein the signed name for a trust group matches the trust group, verifying that the other device sending the trust group membership certificate is a member of the trust group" in (Col 5 lines 1-20).

Response to Arguments

25. Applicant's amendment, filed on Jan. 11, 2007, has Claims 1-20 as original.

26. Applicant's remark, filed on Jan. 11, 2007, argues that neither Hind nor Dondeti teaches or suggests a "trust group membership certificate" for a "trust group comprising a group of devices" such that "when the security-uninitialized device sends the trust group certificate to a branded device ... the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices".

27. Applicant's remark, filed on Jan. 11, 2007, argues that there is no motivation to combine Hind and Dondeti in order to arrive at the above quoted language.

28. Applicant's remark has been fully considered, but found not persuasive based on the reason below.

Regarding to Argument (1):

In regards to Applicant's argument that neither Hind nor Dondeti teaches or suggests a "trust group membership certificate" for a "trust group comprising a group of devices" such that "when the security-uninitialized device sends the trust group certificate to a branded device ... the branded device verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices", Examiner respectfully disagrees. Hind

discloses creating a certificate (i.e., membership certificate) and keys (public and private key) for distribution to a group of users (i.e., group devices), and the certificate is signed an include user group associations and access control groups information as in lines 18-29, Col. 10 from Hind. Dondeti, meanwhile, discloses that any new enrolling host (i.e., uninitialized device) uses the authentication information, such as the capability certificate (i.e., the membership certificate) **[The enrolling host H_1 then sends a message to the sender S, comprising authentication information about itself, the responding SGM's identity 52 and the corresponding keygroup identity 54. The authentication information may be either in the form of a capability certificate 50 (lines 8-12, Col. 5 and Figs. 3 and 4)]** to a sender (i.e., a branded device) so that the sender can verify the new enrolling host identified in the capability certificate is a member of a multicast group (i.e. trusted group) **[The sender S uses the capability certificate 50 to decide whether H_1 is an authorized member of the multicast group. It also checks to see if H_1 has previously requested to join the multicast. This last verification guards against a misbehaving host, trying to join multiple subgroups simultaneously. After the new host's membership is validated, the sender generates message 104 (lines 15-20, Col. 5 and Fig. 3)]**. Therefore, the combination of Hind and Dondeti, contrary to Applicant's argument, discloses the argued "trust group membership certificate" for the trust group such that "when the security-uninitialized device sends the trust group certificate to a branded device ... the branded device

verifies that the security-uninitialized device identified in the trust group membership certificate is a member of the trust group of devices", and the rejection is maintained.

Regarding to Argument (2):

In response to applicant's argument that there is no suggestion or motivation found tin the cited references whereby a person of ordinary skill of the filed of the invention would combine the teachings of the cited references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, since the cited prior art by Hind and Dondeti both disclose the use of certificate for authentication/verification purpose any one of ordinary skill in the art at the time of invention was made to combine the teachings. The motivation for doing so would be to implement the group joining between group members without interposing a central authority as supported by the disclosure from Dondeti that centralized flat scheme consist of a single entity distributing the encryption keys (i.e., central authority) to the group members ... Thus these schemes suffer from the 1 affects n scalability problem (lines 54-58, Col. 1).

Based on the reason above, it is believed that the rejection to the claims should be maintained. Applicant is reminded that additional modification to clarify the claimed limitation is necessary for further consideration.

Conclusion

29. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

a. Mittra (U.S. Patent 5,748,736) disclose a system and method for secure group communication via multicast or broadcast transmission. In preferred embodiments, the system of the invention implements a secure multicast group consisting of senders, receivers, a group security controller (GSC), and at least one trusted intermediary (TI) server. The

GSC and each TI server are responsible for maintaining the security of the group by authenticating and authorizing all other members of the multicast as well as managing the group key(s) (Kgrp(s)) that are used to encrypt the messages multicast to the group. Any member of the group may have more than one role at a time. For example, senders may also be receivers, and the GSC may be combined with one of the senders. Each TI server is a trusted intermediary, which is a special type of sender and receiver. The TI servers create a (logical) hierarchy of secure multicast networks (a secure distribution tree) that makes the system of the invention scalable (able to practically implement a group of any number of members). Some embodiments of the system implement a security protocol supporting data confidentiality, source authentication, data integrity, and sender non-repudiation. Implementation of the system does not require use of any specific security technology (i.e. cryptographic and authentication tools). The decision to use one technology over another is left to the implementor.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Y.C. Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Y.C. Shaw
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100